Enhanced AES-CCMP key structure in IEEE 802.11I

Abstract

This study is conducted to establish an alternative, creative technique for key structure of AES-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) encryption method in IEEE 802.11i. The proposed method modifies AES-CCMP key length from 128 bits to 256 bits through recommending three distinctive solutions including Random Nonce Key, Four Way Handshake alteration and Pseudo Random Function (PRF). Besides, the memory usage and the avalanche effect of the proposed method and the traditional method are compared. The avalanche effect of the proposed method is near to optimized style and the memory usage is approximately close to memory usage of classic AES-CCMP. In addition in the mentioned method, pre computation attack is completely eliminated.